Chapter 14: Installing Fermi Kerberos on a UNIX (non-Linux) System

In this chapter we provide instructions for installing the Fermilab **kerberos** product on a UNIX machine (RH Linux is treated separately in Chapter 15: *Installing Fermi Kerberos on a Linux System*[1]) and for installing Kerberized **ssh**, as the combination works very well. These products are available from *fnkits.fnal.gov.* We describe how to install them using **UPS/UPD**[2]. The information is valid for all supported flavors of UNIX, namely: SunOS, IRIX and OSF1.

14.1 Before You Install Kerberos

14.1.1 Obtain a Kerberos Principal

Strictly speaking, you don't need a Kerberos principal to just install the software. It will be difficult to judge your results without one, however. You'll need to get a principal (plus an initial password) to have access to the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal* for information. Use the online *Request Form for Computing Username and Primary Accounts* at `http://www.fnal.gov/cd/forms/acctreq_form.html`.

14.1.2 Create an Account that Matches your Principal

We strongly recommend that you create an account/login name on the machine that matches the "primary" (the username part) of your user principal. See section C.2 *If your Principal and Login Name do not Match* in Appendix C: *More about Choosing a Principal Name*. Note that even if your login name and principal don't match you can still log into your machine at the console after it's Kerberized, as long as your UNIX password is there.

---

1. The information is also valid for Fermi RedHat Linux, but more options are available for Linux.
2. For documentation on **UPS/UPD**, see `http://www.fnal.gov/docs/products/ups`. Installing products from *fnkits* is described in Part II of the **UPS/UPD** documentation.

14.1.3 Understand your Installation Options

If you don't wish to maintain the **UPS/UPD** software on your machine, we recommend that you install it temporarily in order to install **ssh** and **kerberos**, and then remove it. Instructions for a temporary **UPS/UPD** install are online at `http://www.fnal.gov/docs/products/ups/ReferenceManual/misc/TemporaryInstall.html`.

If you choose not to use **UPS/UPD**, it will be difficult to install the Fermilab **kerberos** product (unless you install via RPM on RH Linux, discussed in Chapter 15: *Installing Fermi Kerberos on a Linux System*). Instead you can download the MIT Kerberos product in a variety of formats from the Web and install it. See Chapter 20: *Installing Kerberos on a non-Fermi-Supported Linux System*.

14.1.4 Install UPS/UPD (Recommended)

If **UPS/UPD** is not already installed on your machine, go ahead and install it (for instructions, see Part III of the *UPS, UPD and UPP v4 Complete Guide and Reference Manual* at `http://www.fnal.gov/docs/products/ups/ReferenceManual/parts.html#partIII`). If your node is not in the fnal.gov domain, make sure that you first register your node for product distribution using the form at `http://www.fnal.gov/cd/forms/upd_registration.html`.

14.1.5 Install Kerberized SSH (Recommended)

Using Kerberized **ssh** with the **kerberos** product in fully strengthened mode smoothes out several operations that can cause extra work in a non-ssh installation. Most importantly, ssh can be configured to always provide encrypted connections. Also, you get X11 connection forwarding so that you don't have to set the $DISPLAY variable, and the X11 connections are encrypted.

As of version 1_2_27, the first Kerberized ssh version, the ssh product components no longer reside in the `/usr/local` directory tree. The newer versions get installed in the `/usr/krb5` directory tree, which should be local to individual machines.

If you have ssh-afs installed from a previous version of ssh, you must remove it in order for the Kerberos, ssh and AFS to work together properly. The new Kerberized versions of ssh know how to work with AFS.

If you've already installed kerberos and want to add Kerberized ssh via UPS/UPD, make sure you run **`ups install-sshd kerberos`** after installing ssh, for reasons discussed below. (The Kerberized ssh RPM can be installed either before or after kerberos.)

Why Install SSH First?

Make sure you install ssh BEFORE you install kerberos (and install the latter in fully-strengthened mode). The UPS kerberos installation checks for the sshd configuration file and, if it exists, makes the appropriate modifications to turn off the authentication methods that shouldn't be allowed, i.e., password and RSA hosts.

The ssh installation, on the other hand, only checks whether an sshd configuration already exists. If so, it simply keeps it, and if not, it creates a default one (a more permissive one). So, if you install ssh after kerberos, you end up with a too-permissive-for-kerberos ssh configuration. This can be fixed by running **`ups install-sshd kerberos`** which invokes the part of the kerberos install script which modifies the sshd configuration.

To Install SSH using UPD

1) First, log in as the appropriate user for product installation (usually *products* or *root*).

2) We recommend that you stop sshd prior to the installation (as *root*):

```
% /etc/rc.d/init.d/sshd stop
```

3) Setup **UPD** by running the command:

```
% setup upd
```

4) Next run the **`upd install`** command to retrieve **ssh** from the product server, and set it as "current" in the database:

```
% upd install ssh [v<N_M>] -G -c
```

5) Log out, if necessary, and log in now as *root* (or **`su`** to *root*).

6) Run the following configuration command (on each individual machine, if installing on a cluster):

```
% ups InstallAsRoot ssh
```

7) Note: The ssh installation sets the values of `RhostsRSAAuthentication`, `RSAAuthentication` and `PasswordAuthentication` in `/etc/sshd_config` to "yes". They must be set to "no"! (`KerberosOrLocalPasswd` must also be "no".) If you proceed to install kerberos, these values will get set

properly. If kerberos is already installed, you must either set the values to "no" by hand, or you can do it by running:

```
% ups install-sshd kerberos
```

8) Restart sshd (as *root*):

```
% /etc/rc.d/init.d/sshd start
```

9) Verify your $PATH is pointing to the right ssh (in case you had an older version of ssh running previously). To test, run the command: **`which ssh`**. It should return `/usr/krb5/bin/ssh`. If not, go into `/usr/bin` and reset the ssh link to `/usr/krb5/bin/ssh`.

Documentation on **ssh** is provided under `http://www.fnal.gov/docs/products/ssh/`.

14.1.6 Do you Need to Allow Incoming Kerberos Connections?

If you plan to log in to your machine over the network and/or offer services, your machine must allow incoming Kerberos connections (including portal mode connections). In this case, you must get a service principal for the host, and one for **FTP** if that is an offered service. These service principal names are of the form `host/<full.node.name>` and `ftp/<full.node.name>` (e.g., `host/mynode.fnal.gov` and `ftp/mynode.fnal.gov`, or for off-site nodes, something like `host/mynode.myuniv.edu` and `ftp/mynode.myuniv.edu`, according to your institution's domain). We also recommend that you get a fixed IP address.

If you need host and ftp principals, first register yourself in the database of system administrators. Go to *System Administrator Registration* at `http://miscomp.fnal.gov/sysadmindb/` to register.

Before installing **kerberos** on a machine the first time, request the host-specific service principals (plus initial passwords) for that machine, using the form at `http://www.fnal.gov/cd/forms/extra_kerb_req_form.html`. You will need to provide the full hostname of the machine.

Notes:

- For a machine with two or more active (static) IP addresses or multiple node names, see section 16.12 *Multiple IP Addresses or Node Names*.
- If you are reinstalling **kerberos** on a machine, you should keep the same host and **FTP** principals. If the `krb5.keytab` is not lost, there's nothing you have to do for these principals. If it is lost, contact *compdiv@fnal.gov* to get passwords reset on the principals.

If you don't intend to allow incoming connections, don't request these service principals, and just answer "no" when asked if you have the passwords for them during installation of the **kerberos** product. You can request and install them at a later date, if needed. To do so, log on as *root* and run the command:

```
% ups install-hostkeys kerberos
```

and provide the passwords as prompted.

14.1.7 Synchronize your Machine with Time Server

When using Kerberos, the client and server must be time-synchronized with each other, each in its local time zone. A wrong system clock is the single most common authentication problem (it typically appears as a "preauthentication failed" message). Use the command **`date -u`** to check the date/time that really counts. Kerberos is configured to allow a discrepancy of five minutes. **xntp** is a product that you can install on your machine to maintain the system time in agreement with Internet standard time servers. It is available from *fnkits* for some platforms[1].

If your system runs AFS, don't install **xntp** or any other synchronizing software; AFS does its own time synchronization. But beware: AFS doesn't set the hardware clock, so, for example, when daylight savings time starts or ends, your clock may be an hour off. Choose ONLY ONE of the following solutions:

- start **xntp**, let it sync the clock, then turn it off
- see if the **afsd** has a **`-nosettime`** option; if so, set it and run **xntp** to handle the timekeeping instead
- (Linux) make sure the date is correct, then run **`/sbin/hwclock --systohc`** to change the hardware clock to match the system clock (or edit your `crontab` to run the above command at some frequency; e.g., to sync it up once a month, add the line `33 3 3 * * /sbin/hwclock --systohc`)

14.1.8 Determine Kerberos Access Mode(s)

Before installing you must first determine whether you want **kerberos** configured in fully strengthened mode, in mixed mode (Kerberos plus **ssh**), or in a customized mode.

---

1. If your node is not in the fnal.gov domain, make sure that you first register your node for product distribution via fnkits using the form at `http://www.fnal.gov/cd/forms/upd_registration.html` .

Fully Strengthened Mode (Kerberos Only)

This mode enables only Kerberized access to the node. This includes Kerberized ssh. It disables *all* non-Kerberized means of accessing the node. This is the mode on-site Kerberized systems are obliged to choose beginning Jan. 1, 2002.

Mixed Mode (Kerberos plus SSH)

This mode enables Kerberized access to this node, does not disable any existing non-Kerberized **ssh** access to the node, but disables *all other* non-Kerberized means of accessing the node. This mode is incompatible with Kerberized **ssh**.

For ON-SITE SYSTEMS, this mode is not in compliance with the Computing Policy, and thus is NOT ALLOWED as of January 1, 2002.

Other

If neither of these configurations applies, read the file `README.INSTALL.DETAILS` which describes all of the possible installation options in detail.

This is recommended only for experts.

14.1.9 Choose Login Program

Secondly, you can choose to use the standard UNIX login program or to install the Kerberos login program[1]. As of September 2001 the installation of Fermi **kerberos** automatically replaces the system login program with the Kerberized version. The Kerberos login program is required for CRYPTOCard support.

14.2 Installing Fermi Kerberos using UPS/UPD

The Fermilab **kerberos** product is preconfigured and in general should require no further actions beyond the installation instructions found here (this information has been taken from its `README.INSTALL` file). **kerberos**

1. Not applicable to IRIX systems or to Linux or Solaris if using the GUI login box; the login program isn't run in these cases.

must be properly installed on each individual node. For more information, or to do a custom install, see the the various README files that come with the product.

1) First, log in as the appropriate user for product installation (usually *products* or *root*).

2) Setup **UPD** by running the command:

```
% setup upd
```

3) Next run the **`upd install`** command to retrieve **kerberos** from the product server, and set it as "current" in the database[1]:

```
% upd install kerberos [v<N_M>] -G -c
```

4) Log out, if necessary, and log in now as *root* (or **`su`** to *root*).

5) Choose the configuration option appropriate to your situation (as described in section 14.1.8 *Determine Kerberos Access Mode(s)*) and issue the corresponding **`ups install`** command (note the **`ups`** in place of the **`upd`**) to complete the installation of the **kerberos** product. You need to include the version (**`v<N_M>`**) only if **kerberos** has not been declared as "current". (See section 16.1 *Alterations Made to your System when Fermi Kerberos is Installed* for information on what changes this portion of the installation makes to your system.)

   a) For fully strengthened mode (required for on-site systems):
   `ups install kerberos [v<N_M>]`

   b) For mixed mode (allowed for off-site systems):
   `ups install-keep-ssh kerberos [v<N_M>]`

   c) For any other configuration, refer to the file
   `README.INSTALL.DETAILS` (recommended for experts only)

6) If you wish to override the standard UNIX login program on the machine with a Kerberized login program as discussed in section 14.1.9 *Choose Login Program*, issue the command:

```
% ups install-login kerberos [v<N_M>]
```

   where **`v<N_M>`** is not needed if the **kerberos** product is chained to "current".

7) If you had installed **kerberos** v0_1 or v0_2 and are now reinstalling **kerberos** on the node, you need to clean out the files which had been copied to `/usr/local` (and are now copied to `/usr/krb5`). To so

1. Running the **`upd install`** command just puts the kerberos files in the products area. At this point you can run **`setup kerberos`** and you can get Kerberized network connections or do password maintenance. You cannot yet do any thing requiring a host key.

so, run the command:

```
% ups clean kerberos [v<N_M>]
```

where **v<N_M>** refers to the newly installed version, and is not needed if the new version is chained to “current”.

Also, if you are reinstalling, keep the same host and FTP service principals to reuse the identity of the machine.